

UNCLASSIFIED	CONFIDENTIAL	SECRET
--------------	--------------	--------

OLC

## EXECUTIVE SECRETARIAT

### Routing Slip

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	D/DCI/IC				
4	DDS&T				
5	DDI				
6	DDA				
7	DDO				
8	D/DCI/NI				
9	GC				
10	LC				
11	IG				
12	Compt				
13	D/Pers				
14	D/S				
15	DTR				
16	Asst/DCI				
17	AO/DCI				
18	C/IPS				
19	DCI/SS				
20	D/EE0				
21	1. 177777				
22	1. 177777				

ILLEGIB

SUSPENSE \_\_\_\_\_ Date \_\_\_\_\_

Remarks:

25X1

Executive Secretary

26 JUL 77

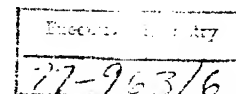
Date

3637 (7-76)

NSC review completed.

## THE WHITE HOUSE

WASHINGTON



April 25, 1977

## MEMORANDUM FOR

THE VICE PRESIDENT  
THE SECRETARY OF STATE  
THE SECRETARY OF DEFENSE  
THE ATTORNEY GENERAL  
THE DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Foreign Intelligence Electronic Surveillance Legislation

The President has reached the following decisions concerning foreign intelligence electronic surveillance legislation:

1. The basic structure of the bill should be as recommended by the Attorney General's PRM/NSC-11 Subcommittee report and endorsed by the SCC.
2. The report's recommendations on issues 1, 4, 5, 6 and 7 are accepted as endorsed by the SCC.
3. Concerning issue 2 in the report, the current electronic surveillance bill should not cover U.S. persons abroad. However, a statement should be made at the time of its introduction that the Department of Justice will proceed to draft a separate bill to extend legal safeguards to Americans overseas who are targeted for electronic surveillance for either intelligence or law enforcement purposes.
4. Concerning issue 3, warrants will be required for all electronic surveillance activities conducted within the U.S. However, the warrant requirement for surveillances directed against foreign powers will allow for substantially longer periods of time before reauthorization and application requirements will be designed to reduce the amount of sensitive information that will be transmitted to the judges (Option C with Justice Department recommended changes).

The Attorney General's Subcommittee should now assume responsibility for introduction of the Administration's bill in Congress and act as a tactical steering group while the bill is under consideration. Any significant proposed changes to the bill should, however, be referred to the SCC for consideration.

Zbigniew Brzezinski

## A BILL

To amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1977".

SEC. 2. Title 18, United States Code, is amended by adding a new chapter after chapter 119 as follows:

"Chapter 120. -- ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

"Sec.

"2521. Definitions.

"2522. Authorization for electronic surveillance for foreign intelligence purposes.

"2523. Designation of judges authorized to grant orders for electronic surveillance.

"2524. Application for an order.

"2525. Issuance of an order.

"2526. Use of information.

"2527. Report of electronic surveillance."

§ 2521. Definitions

"(a) Except as otherwise provided in this section the definitions of section 2510 of this title shall apply to this chapter.

"(b) As used in this chapter --

"(1) 'Foreign power' means --

"(A) a foreign government or any component thereof, whether or not recognized by the United States;

"(B) a faction of a foreign nation or nations, not substantially composed of United States persons;

"(C) an entity, which is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

"(D) a foreign-based terrorist group;

"(E) a foreign-based political organization, not substantially composed of United States persons; or

"(F) an entity which is directed and controlled by a foreign government or governments.

"(2) 'Agent of a foreign power' means --

"(A) a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), who --

"(i) knowingly engages in clandestine intelligence activities for or on behalf of a foreign power, or activities in furtherance thereof, which activities involve or will involve a violation of the criminal statutes of the United States;

"(ii) knowingly engages in activities that involve or will involve sabotage or terrorism for or on behalf of a foreign power;

"(iii) knowingly collects or transmits information or material pursuant to the direction of an intelligence service or intelligence network of a foreign power in a manner intended to conceal the nature of such information or material or the fact of such transmission or collection, under circumstances which indicate the transmission of such information or material may be harmful to the security or foreign policy of the United States; or

"(iv) conspires with or knowingly aids or abets any person engaged in activities described in subsections A(i)-(iii) above.

"(B) any person, other than a United States citizen or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), who --

"(i) is an officer or employee of a foreign power;

"(ii) is engaged in clandestine intelligence activities or activities that involve or will involve sabotage, or terrorism for or on behalf of a foreign power; or

"(iii) conspires with or knowingly aids or abets a person described in paragraph (ii) above or subsections A(i)-(iii).

"(3) 'Terrorism' means activities which --

"(A) are violent acts or acts dangerous to human life which would be criminal under the laws of the United States or of any State if committed within its jurisdiction; and

"(B) appear to be intended --

"(i) to intimidate or coerce the civilian population, or

"(ii) to influence the policy of a government by intimidation or coercion.

"(4) 'Sabotage' means activities which would be prohibited by title 18, United States Code, chapter 105, if committed against the United States.

"(5) 'Foreign intelligence information' means --

"(A) information which relates to, and is deemed necessary to the ability of the United States to protect itself against, actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

"(B) information with respect to a foreign power or foreign territory, which relates to, and is deemed necessary to:

"(i) the national defense or the security of the Nation; or

"(ii) the successful conduct of the foreign affairs of the United States;

"(C) information which relates to, and is deemed necessary to the ability of the United States to protect against terrorism by a foreign power or an agent of a foreign power;

"(D) information which relates to, and is deemed necessary to the ability of the United States to protect against sabotage by a foreign power or an agent of a foreign power; or

"(E) information which relates to, and is deemed necessary to the ability of the United States to protect against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power;

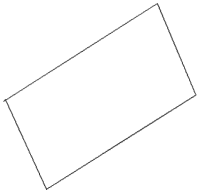
"(6) 'Electronic surveillance' means --

"(A) the acquisition by an electronic; mechanical, or other surveillance device of the contents of any wire or radio/communication sent by or intended to

be received by a particular, known United States person in the United States without the consent of any party thereto, where the contents are acquired by intentionally targeting that United States person, under circumstances in which a warrant would be constitutionally required if the surveillance was not for foreign intelligence purposes;

NSA  
"(B) the acquisition by an electronic, mechanical, or other surveillance device, of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, where such acquisition occurs in the United States while the communication is being transmitted by wire;

"(C) the intentional acquisition, by an electronic, mechanical, or other surveillance device, of the contents of any radio communication, without the consent of any party thereto, made under circumstances in which a warrant would be constitutionally required if the surveillance was not for foreign intelligence purposes, and where both the sender and all intended recipients are located within the United States; or



"(D) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a warrant would be constitutionally required if the surveillance was not for foreign intelligence purposes.

ILLEGIB

"(7) 'Attorney General' means the Attorney General of the United States (or Acting Attorney General) or an Assistant Attorney General specially designated in writing by the Attorney General.

"(8) 'Minimization procedures' means procedures which are reasonably designed to minimize the acquisition, retention, and dissemination of any information concerning United States persons without their consent that does not relate to the ability of the United States --

"(A) to protect itself against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

"(B) to provide for the national defense or security of the Nation;

"(C) to provide for the conduct of the foreign affairs of the United States;

"(D) to protect against terrorism by a foreign power or an agent of a foreign power;

"(E) to protect against sabotage by a foreign power or an agent of a foreign power; or

"(F) to protect against the clandestine intelligence activities of an intelligence service or network of a foreign power or an agent of a foreign power;

and which are reasonably designed to insure that information which relates solely to the conduct of foreign affairs shall not be maintained in such a manner as to permit the retrieval of such information by reference to a United States person.

who was a party to a communication acquired pursuant to this chapter; and if the target of the electronic surveillance is a foreign power which qualifies as such solely on the basis that it is an entity controlled and directed by a foreign government or governments, and unless there is probable cause to believe that a substantial number of the officers or executives of such entity are officers or employees of a foreign government, or agents of a foreign power as defined in section 2521(b)(2)(B), procedures which are reasonably designed to prevent the acquisition, retention,

and dissemination and to require the expunging of communications of United States persons who are not officers or executives of such entity responsible for those areas of its activities which involve foreign intelligence information.

"(9) 'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence or a corporation which is incorporated in the United States, but not including corporations which are foreign powers.

"(10) 'United States' when used in a geographic sense means all areas under the territorial sovereignty of the United States, the Trust Territory of the Pacific Islands, and the Panama Canal Zone.

"§ 2522. Authorization for electronic surveillance for  
foreign intelligence purposes

" Applications for a court order under this chapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to Federal judges having jurisdiction under section 2523 of this chapter, and a judge to whom an application is made may grant an order, in conformity with section 2525 of this chapter, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.

"§ 2523. Designation of judges authorized to grant orders  
for electronic surveillance

"(a) The Chief Justice of the United States shall publicly designate seven district court judges, each of whom shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under

the procedures set forth in this chapter, except that no judge designated under this subsection shall have jurisdiction of an application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the special court of review established in subsection (b).

"(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a special court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such special court determines that the application was properly denied, the special court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

"(c) Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be sealed and maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

"§ 2524. Application for an order

"(a) Each application for an order approving electronic surveillance under this chapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 2523 of this chapter. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this chapter. It shall include the following information --

"(1) the identity of the Federal officer making the application;

"(2) the authority conferred on the applicant by the President of the United States and the approval of the Attorney General to make the application;

"(3) the identity or a description of the target of the electronic surveillance;

what detail?

"(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that --

"(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power;  
and

"(B) the facilities or the place at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power;

"(5) a statement of the proposed minimization procedures;

"(6) when the target of the surveillance is not a foreign power as defined in section 2521(b)(1)(A), (B) or (C), a factual description of the nature of the information sought;

"(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate --

"(A) that the information sought is foreign intelligence information;

"(B) that the purpose of the surveillance is to obtain foreign intelligence information;

"(C) that such information cannot feasibly be obtained by normal investigative techniques;

"(D) including a designation of the type of foreign intelligence information being sought according to the categories described in section 2521(b)(5);

"(E) when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), including a statement of the basis for the certification that --

"(i) the information sought is the type of foreign intelligence information designated; and

"(ii) such information cannot feasibly be obtained by normal investigative techniques;

"(F) when the target of the surveillance is a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), stating the period of time for which the surveillance is required to be maintained;

"(8) when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), a statement of the means by which the surveillance will be effected;

"(9) a statement of the facts concerning all previous applications that have been made to any judge under this chapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and

"(10) when the target of the surveillance is not a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), a statement of the period of time for which the electronic surveillance is required to be maintained.

If the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this chapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

"(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

"(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 2525 of this chapter.

"§ 2525. Issuance of an order

"(a) Upon an application made pursuant to section 2524 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that --

"(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

"(2) the application has been made by a Federal officer and approved by the Attorney General;

"(3) on the basis of the facts submitted by the applicant there is probable cause to believe that --

"(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

"(B) the facilities or place at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power; |

"(4) the proposed minimization procedures meet the definition of minimization procedures under section 2521(b)(8) of this title;

"(5) the application which has been filed contains the description and certification or certifications, specified in section 2524(a)(7) and, if the target is a United States person, the certification or certifications are not arbitrary or capricious on

the basis of the statement made under section  
2524(a)(7)(E):

"(b) An order approving an electronic surveillance under  
this section shall --

"(1) specify --

"(A) the identity or a description of  
the target of the electronic surveillance;

"(B) the nature and location of the facilities  
or the place at which the electronic surveillance  
will be directed;

"(C) the type of information sought to be  
acquired;

"(D) when the target of the surveillance is  
not a foreign power, as defined in section 2521  
(b)(1)(A), (B), or (C), the means by which the  
electronic surveillance will be effected; and

"(E) the period of time during which the elec-  
tronic surveillance is approved; and

"(2) direct --

"(A) that the minimization procedures be  
followed;

"(B) that, upon the request of the applicant,  
a specified communication or other common carrier,  
landlord, custodian, contractor, or other specified

person furnish the applicant forthwith any and all information, facilities, or technical assistance, necessary to accomplish the electronic surveillance in such manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, contractor, or other person is providing that target of electronic surveillance; and

"(C) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

"(c) An order issued under this section may approve an electronic surveillance not targeted against a foreign power, as defined in section 2521(b)(1)(A), (B), or (C), for the period necessary to achieve its purpose, or for ninety days, whichever is less; an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 2521(b)(1)(A), (B), or (C) for the period specified in the certification required in section 2524(a)(7)(F), or for one year, whichever is less. Extensions of an order issued under this chapter may be granted on the same basis as an original order upon an application for an extension made in the same manner

as required for an original application and after new findings required by subsection (a) of this section. In connection with the new findings of probable cause, the judge may require the applicant to submit information obtained pursuant to the original order or to any previous extensions, or any other information or evidence as he finds necessary to make such new findings.

"(d) Notwithstanding any other provision of this chapter when the Attorney General reasonably determines that --

"(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained, and

"(2) the factual basis for issuance of an order under this chapter to approve such surveillance exists, he may authorize the emergency employment of electronic surveillance if a judge designated pursuant to section 2523

of this chapter is informed by the Attorney General or his designate at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this chapter is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such acquisition. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this chapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated without an order having been issued, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee or other authority of the United States,

a State or a political subdivision thereof. A denial of the application made under this subsection may be reviewed as provided in section 2523.

"§ 2526. Use of information

"(a) Information concerning United States persons acquired from an electronic surveillance conducted pursuant to this chapter may be used and disclosed by Federal officers and employees only for purposes specified in section 2521(b)(8)(A)-(F), or for the enforcement of the criminal law. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

"(b) The minimization procedures required under this chapter shall not preclude the retention and disclosure, for law enforcement purposes, of any information which constitutes evidence of a crime if such disclosure is accompanied by a statement that such evidence, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

"(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, or other authority of the United States, any information obtained or derived from an electronic surveillance, the Government shall prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use the information or submit it in evidence notify the court in which the information is to be disclosed or used or, if the information is to be disclosed or used in or before another authority, shall notify a court in the district wherein the information is to be so disclosed or so used that the Government intends to so disclose or so use such information. Whenever any court is so notified, or whenever a motion is made pursuant to § 3504 of this title, or any other statute or rule of the United States to suppress evidence on the grounds that it was obtained or derived from an unlawful electronic surveillance, the court, or where the motion is made before another authority, a court in the same district as the authority, shall, if the Government by affidavit asserts that an adversary hearing would damage the national security or the foreign relations of the United States, review in camera and ex parte the application, order, and transcript of the surveillance to

determine whether the surveillance was authorized and conducted in a manner that did not violate any right afforded by the Constitution and statutes of the United States to the person aggrieved; provided that, in making this determination, the court may disclose to the aggrieved person portions of the application, order, or transcript only in compelling situations where the harm to national security is outweighed by the requirements of due process in that particular case. If the court determines that the electronic surveillance of the person aggrieved was conducted unlawfully, the court shall suppress that information which was obtained or derived unlawfully from the electronic surveillance of the person aggrieved.

"(d) If an emergency employment of the electronic surveillance is authorized under section 2525(d) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of --

"(1) the fact of the application;

"(2) the period of the surveillance; and

"(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

"§ 2527. Report of electronic surveillance

"In April of each year, the Attorney General shall report to the Administrative Office of the United States Courts and shall transmit to Congress with respect to the preceding calendar year --

"(1) the number of applications made for orders and extensions of orders approving electronic surveillance;

"(2) the number of such orders and extensions granted, modified, and denied; and

"(3) the number of such surveillances terminated during the preceding year.

*I would like to see the results of a sample report by the AG for 1976 (actual cases):*

*a - as were actually handled (all 90-day requests and 90-day renewals, and*

*b - if the cases were as stipulated in the Bill (wholly foreign intelligence requests, upon original application, were approved for one year).*

SEC. 3. The provisions of this Act and the amendment made hereby shall become effective upon enactment: Provided, That, any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of chapter 120, title 18, United States Code, if that surveillance is terminated or an order approving that surveillance is obtained under this chapter within ninety days following the designation of the first judge pursuant to section 2523 of chapter 120, title 18, United States Code.

SEC. 4. Chapter 119 of title 18, United States Code, is amended as follows:

(a) Section 2511(1) is amended --

(1) by inserting "or chapter 120 or as otherwise authorized by a search warrant or order of a court of competent jurisdiction," immediately after "chapter" in the first sentence;

(2) by inserting a comma and "or, under color of law, willfully engages in any other form of electronic surveillance as defined in chapter 120" immediately before the semicolon in paragraph (a);

(3) by inserting "or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120" immediately after "contents of any wire or oral communication" in paragraph (c);

(4) by inserting "or any other form of electronic surveillance, as defined in chapter 120," immediately before "in violation" in paragraph (c);

(5) by inserting "or information obtained under color of law by any other form of electronic surveillance as defined in chapter 120" immediately after "any wire or oral communication" in paragraph (d);  
and

(6) by inserting "or any other form of electronic surveillance, as defined in chapter 120," immediately before "in violation" in paragraph (d).

(b)(1) Section 2511(2)(a)(i) is amended by inserting the words "or radio communication" after the words "wire communication" and by inserting the words "or otherwise acquire" after the word "intercept."

(2) Section 2511(2)(a)(ii) is amended by inserting the words "or chapter 120" after the second appearance of the word "chapter," and by striking the period at the end thereof and adding the following: "or engage in electronic surveillance, as defined in chapter 120: Provided, however, That before the information, facilities, or technical assistance may be provided, the investigative or law enforcement officer shall furnish to the officer, employee, or agency of the carrier either --

"(1) an order signed by the authorizing judge certifying that a court order directing such assistance has been issued; or

"(2) in the case of an emergency interception or electronic surveillance as provided for in section 2518(7) of this chapter or section 2525(d) of chapter 120, a sworn statement by the investigative or law enforcement officer certifying that the applicable statutory requirements have been met, and setting forth the period of time for which the electronic surveillance is authorized and describing the facilities from which the communication is to be acquired. Any violation of this subsection by a communication common carrier or an officer, employee, or agency thereof, shall render the carrier liable for the civil damages provided for in section 2520."

(c)(1) Section 2511(2)(b) is amended by inserting the words "or otherwise engage in electronic surveillance, as defined in chapter 120," after the word "radio."

(2) Section 2511(2)(c) is amended by inserting the word "or engage in electronic surveillance, as defined in chapter 120," after the words "oral communication" and by inserting the words "or such surveillance" after the last word in the paragraph and before the period.

(3) Section 2511(2) is amended by adding at the end of the section the following provision:

"(e) Notwithstanding any other provision of this title or sections 605 or 606 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance as defined in section 2521 (b)(6) of chapter 120 without a court order for the sole purpose of:

"(i) testing the capability of electronic equipment, provided that the test period shall be limited in extent and duration to that necessary to determine the capability of the equipment, that the content of any communication acquired under this paragraph shall be retained and used only for the purpose of determining the capability of such equipment, shall be disclosed only to the persons conducting the test, and shall be destroyed upon completion of the testing, and that the test may exceed ninety days only with the prior approval of the Attorney General; or

capability of electronic surveillance equipment being used unlawfully, provided that such electronic surveillance shall be limited in extent and duration to that necessary to determine the existence and capability of such equipment, and that any information acquired by such surveillance shall be used only to enforce this chapter or section 605 of the Communications Act of 1934 or to protect information from unlawful electronic surveillance."

(d) Section 2511(3) is repealed; provided that, nothing contained in chapter 119 of title 18, United States Code, or section 605 of the Communications Act of 1934 (47 U.S.C. § 605) shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international communications by a means other than electronic surveillance as defined in section 2521(b)(6) of title 18, United State Code, as amended by this Act, and the procedures in chapters 119 and 120 of title 18, United States Code, as amended by this Act, shall be the exclusive means by which electronic surveillance, as defined in section 2521(b)(6) of chapter 120, and the interception of wire

and oral communications, as defined in section 2510 of chapter 119, may be conducted within the United States.

(e) Section 2515 is amended by inserting the words "or electronic surveillance as defined in chapter 120, has been made" after the word "intercepted" and by inserting the words "or other information obtained from electronic surveillance, as defined in chapter 120," after the second appearance of the word "communication".

(f) Section 2518(1) is amended by inserting the words "under this chapter" after the word "communication".

(g) Section 2518(4) is amended by inserting the words "under this chapter" after both appearances of the words "wire or oral communication".

(h) Section 2518(9) is amended by striking the word "intercepted" and inserting the words "intercepted pursuant to this chapter" after the word "communication".

(i) Section 2518(10) is amended by striking the word "intercepted" and inserting the words "intercepted pursuant to this chapter" after the first appearance of the word "communication".

(j) Section 2519(3) is amended by inserting the words "pursuant to this chapter" after the words "wire or oral communications" and after the words "granted or denied".

(k) Section 2520 is amended by deleting all before subsection (2) and inserting in lieu thereof: "any person other than a foreign power or an agent of a foreign power as defined in sections 2521(b)(1) and 2521(b)(2)(B) of chapter 120, who has been subject to electronic surveillance, as defined in chapter 120, or whose wire or oral communication has been intercepted, or about whom information has been disclosed or used, in violation of this chapter, shall (1) have a civil cause of action against any person who so acted in violation of this chapter and".